Pertanika J. Sci. & Technol. 29 (4): 3081 - 3098 (2021)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

A Privacy Preserving Framework for Health Records using Blockchain

Chitra Karunakaran, Kavitha Ganesh*, Sonya Ansar and Rohitha Subramani

Department of Information Technology, BSA Crescent Institute of Science & Technology, Chennai 600045, India

ABSTRACT

Electronic Health Records (EHR) is the electronic form of storing a patient's medical history. EHR contains patient's data such as progress notes, medications, prescriptions, vital signs, scan reports and laboratory data. Transferring EHR over the internet improves the quality of health care and reduces medical costs. However, in the traditional system, the EHR are stored across different decentralised hospitals, making data sharing difficult and increasing the risk of patient privacy. A privacy-preserving framework for electronic health records using blockchain technology is implemented to address these issues. The patient has complete control over the EHR, and the patient can share their health records with doctors of various medical institutions. The privacy and security of the patient's EHR are guaranteed by the verifiability and immutability property of the blockchain technology. The doctor upload the EHR, and it is encrypted using the SHA256 hashing algorithm and stored as a separate block. The patient shares the EHR with the doctor of any medical institution through the unique key shared via the doctor's email. The doctor can access and update the EHR using the shared key. The block validation is done using Delegated Proof of Stake (DPoS) consensus algorithm, which guarantees the privacy of the patient's data. The proposed system based on the DPoS algorithm has considerabe reduction in resource utilisation, computational capacity, time, and cost for EHR transactions.

Keywords: Blockchain, delegated proof of stake, electronic health records, healthcare, privacy, SHA256

ARTICLE INFO

Article history:
Received: 28 May 2021
Accepted: 9 August 2021
Published: 28 October 2021

DOI: https://doi.org/10.47836/pjst.29.4.45

E-mail addresses:
chitraashwin9896@gmail.com (Chitra Karunakaran)
gkavitha.78@gmail.com (Kavitha Ganesh)
sonya.yasmin152@gmail.com (Sonya Ansar)
srohitha23@gmail.com (Rohitha Subramani)
*Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

INTRODUCTION

Electronic Health Records (EHR) are digital health records of a patient created and managed by a medical practitioner or a staff in a health care organisation. EHR contains treatment given, medical history about a patient, and scan reports. Medical records of a patient are very useful because the doctors need to know the complete medical history of the patient prior to treatment in order to provide effective treatment. However, the patient cannot carry all the medical records every time they visit a doctor for consultation (Xia et al., 2017). It is convenient for both patients and doctors when the medical records are stored as EHR and transferred over the network to the doctor (Guo et al., 2018). The EHR is shared with doctors anywhere in the world, which makes the patient get consulted by the best doctors globally. However, maintaining the patient's data security and privacy are important as the data are transferred over the internet (Liu et al., 2018). Currently, the EHR is stored across different decentralised hospitals that make data sharing difficult with concern on patient privacy (Vedi et al., 2019). Blockchain is an efficient way to store and transfer data through the internet to guarantee privacy and security. In the healthcare sector, EHR plays a vital role in providing effective treatment, but it has to consider the privacy and security of patient data (Dagher et al., 2018). Blockchain has been implemented in many healthcare organisations for secure storage and transfer of medical data to monitor the complete shipping of drugs and store the shipping data (Wang et al., 2018).

Blockchain technology is a list of blocks where data is hashed and linked to the next block (Kadam et al., 2019). The data are hashed using a hashing algorithm such as MD, MD2, MD4, MD5, MD6, SHA1, SHA256, SHA3. The previous block's hash is linked to the next block, so, it cannot be changed once data is recorded, which provides immutability. If a hacker wants to change data in a particular block, then the corresponding hash value changes so the hacker has to change all the hash values of the blocks present after the modified block. It results in the wastage of computing power and cost for the hacker. The data blocks are replicated and stored in different decentralised nodes of a network (Zubaydi et al., 2019).

Blockchain is a decentralised network with peer to peer nodes, and there is no authorised node that decides (Christidis & Devetsikiotis, 2016). All the transactions in the blockchain are secure and verified using the consensus algorithm. Blockchain uses a consensus algorithm to reach an agreement and ensure the consistency and reliability of data (Alhaqbani & Fidge, 2008). The objective of the consensus algorithm is to provide an equal right to every node, mandatory participation of every node on reaching an agreement.

There is around 30 consensus algorithm that has been found in literature and some algorithms widely used are Proof of Work (PoW), Proof of Stake (PoS) and Proof of Delivery (PoD) (Tasatanattakool & Techapanupreeda, 2018). However, the Delegated Proof of Stake (DPoS) consensus algorithm is implemented in the proposed framework because DPoS is more efficient, highly scalable and requires less energy than Proof of Work (Yang et al., 2018).

There are sensor-based health monitoring systems in which data generated by the Internet of Things (IoT) devices provide information about the patient's health condition (Guo et al., 2018). However, this method of gathering information would be difficult for the patients as they have to wear sensors 24/7. Furthermore, the sensor data are not highly reliable, and patients always prefer to meet the doctors for consultation in person. Here, the hospital maintains the health records, and the records can be accessed only by the doctors of that particular hospital. So, suppose a patient wants to consult a doctor of another medical institution. It is impossible to share those data with the expert doctors available in other hospitals and other countries.

The health care domain is improving using advanced technologies like blockchain, AI, and Machine learning (Ahram et al., 2017). In this work, a privacy-preserving framework using blockchain is developed, and it ensures the transfer of EHR with guaranteed privacy. Furthermore, the SHA256 algorithm is implemented for data encryption and Delegated Proof of Stack (DPoS) consensus algorithm is used for the secure transaction of EHR.

The rest of the paper is structured as follows: section 2 discusses the relevant literature related to this problem. Section 3 discusses the methodology of a privacy-preserving framework for EHR, and section 4 presents the results and performance analysis of the proposed framework. Finally, section 5 presents the conclusion and future work.

LITERATURE SURVEY

Many papers have discussed the privacy issues of EHR. Guo et al. (2018) have discussed a secure attribute-based signature scheme with multiple authorities for blockchain in Electronic Medical Records (EMR). In this paper, the EMR is stored in a separate server. There are many authorities among which data can be shared, such as hospitals, insurance companies, and medical research institute. Patients create, manage, control and sign their own EMR and share their data with any authority like doctors and insurance companies. The proposed work combines both blockchain and attribute-based schemes to share EMR records among multiple authorities. Each authority has a private key to view the data. The main advantage is that it supports multiple authorities and resists collision attacks on a cryptographic hash that finds two inputs producing the same hash value. The disadvantage of the system is that the cost and performance depend on the number of authorities.

Hossein et al. (2019) have proposed a blockchain-based privacy-preserving healthcare architecture. Sensors are attached to the patient’s body to gather blood pressure, heart rate, and ECG information. The data is transmitted through Bluetooth to the mobile phone or PDA of the patient. Hash and cryptographic operations are performed, and the miner creates a block. The blocks are verified using the Proof of Work (PoW) consensus algorithm.

Healthcare institutions are responsible for registering the patient and allocating a cluster miner to each patient. This work provides a high level of confidentiality, integrity and security. However, the problem is that the patients cannot wear the sensors 24/7, and the wearable sensors are not cost-effective.

Chen et al. (2019) have discussed blockchain-based secure storage for medical records and medical service frameworks. The three leading authorities in accessing medical data storage are the doctor, patient and third parties such as insurance companies. Data must be stored securely and shared between these authorities safely. The authors have proposed a framework to store and transfer EHR securely using blockchain and cloud technology. The blockchain uses a peer-peer propagation method to share resources such as medical data through a consensus algorithm. The medical records are not shared without the permission of the patient. The scheme does not depend on any third party such as a Healthcare care manager, admin and no single party has the authority to affect the processing of medical data, which is the main advantage of this work. Furthermore, the PoW consensus algorithm is implemented, which increases computational power, energy consumption and cost.

An enhanced architecture for privacy-preserving data integration in a medical research environment has been proposed by Jabeen et al. (2017). The reversible pseudonym technique is used in which artificial identifiers replace data records. In this scheme, a trusted third party generates a pseudonym termed Global Identifiers (GID). The GID allows linking patient's medical records from different hospitals. If a patient changes a care provider or hospital, all the medical records can still be linked, and the patient history is created. Thus, the patient health record can be revived as the medical records are not stored in any medical institution. The drawback of this approach is that there is a possibility of compromising the health records' privacy if the GID of a patient is known to attackers.

Blockchain-based personal data protection using a decentralised approach has been discussed by Zyskind et al. (2015). In this proposed approach, the patients are authorised to own and control their data. This framework provides full transparency to the user to view what is being done with the data and who accesses the data. This work implements a protocol that turns a blockchain into an automated access control manager and does not require trust in a third party. Only patients can change the user's permission in accordance with access control policies. All the nodes are equally trusted, and decision making is a collective process that leads to Sybil attacks, high latency and energy consumption.

All the above stated issues of the existing privacy-preserving models have been resolved in the proposed framework. As a result, the EHR can be shared across medical institutions globally with guaranteed privacy. In addition, the Delegated Proof of Stake (DPoS) consensus algorithm implemented in this work is efficient in energy consumption and cost compared to the other consensus algorithms like PoW and PoS.

METHODOLOGY

The health records of patients are generally managed by health care service providers and medical institutions. A privacy-preserving data sharing framework using blockchain is implemented in this work to assure data privacy in EHR. In the proposed framework, the patient has complete control over the EHR and can transfer the data to any doctor he visits, even outside the medical institution. The sensitive data are stored as blocks, and blockchain improves the transparency and immutability of the stored data in a decentralised network. Furthermore, the blockchain is a secured and trusted architecture and different consensus algorithms are implemented based on the application of domain-specific requirements (Zubaydi et al., 2019).

The proposed Privacy-Preserving Data Sharing Framework for EHR is depicted in Figure 1. The major components of this framework are User Authentication, Block Creation, Block Validation and Record Transaction. As a first step, the patient and the doctor get registered to the e-health centre. Then, when a patient consults a doctor, the EHR that contains information such as treatment given, medical history about the patient, scan reports, and prescribed medicines are been generated by the doctor. The doctor then uploads the EHR to the webpage of the e-health centre. Next, the EHR is encrypted using the SHA256 hashing algorithm, and it will be stored as a separate block. Finally, the block ID is sent to both doctor and patient.

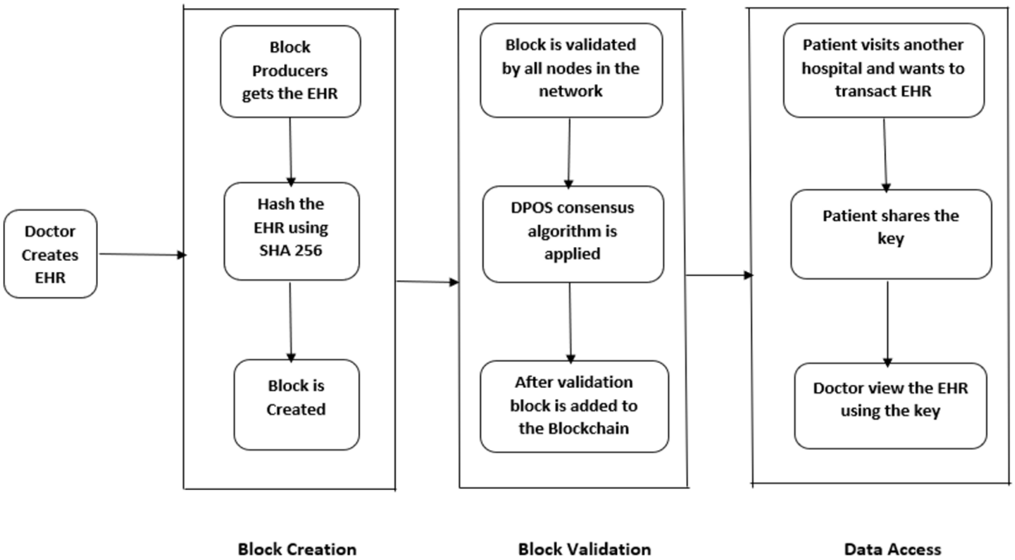

Doctor Creates EHR
Block Producers gets the EHR
Hash the EHR using SHA 256
Block is Created
Block is validated by all nodes in the network
DPOS consensus algorithm is applied
After validation block is added to the Blockchain
Patient visits another hospital and wants to transact EHR
Patient shares the key
Doctor view the EHR using the key
Block Creation
Block Validation
Data Access

Figure 1. Privacy-Preserving Data Sharing Framework for EHR

Then a block is created by the transition node, and the hash value is generated for the current block using the SHA256 hashing algorithm (Shen et al., 2019). The hash value of the previous block is added to provide immutability, and the block is created. The block is then validated using Delegated Proof of Stake (DPoS) consensus algorithm. After validation, the block is added to the blockchain. In the proposed framework, the patient has complete control over accessing the EHR. Therefore, if a patient visits another doctor and consult with the previous health records, he can transfer the health record to any doctor through the e-health centre. The patient EHR are shared to the doctor's mail id through a One-Time Password (OTP). The doctor is now permitted to log in, and using the generated OTP, the doctor can view the patient's Electronic Health Record.

The implementation of blockchain technology over the traditional system of storing and retrieving EHR increases the system's efficiency, reduces the risk of loss of EHR and avoids modification of information in EHR (Jin et al., 2019). The Delegated Proof of Stake (DPoS) consensus algorithm is employed over the Proof of Work (PoW) consensus algorithm due to the computational power and energy reduction. The DPoS consensus algorithm provides faster transactions than PoW and is also environmentally friendly (Judith et al., 2018).

A: User Authentication

The doctor and the patient are registered in the user authentication module by providing their name, mail ID, and contact number. The details are stored using the MySQL database. The user authentication process is shown in Figure 2. When a doctor or the patient logs in, the username and password are validated by fetching details from the database. If the username and password are correct, the homepage is displayed, or an error message is displayed. The doctor has a separate home page and performs tasks like viewing and updating EHR. The patient has a separate home page and has access permissions to share and view EHR. After authentication, the patients and doctors are allowed to access the web page of the e-health centre. The algorithm implemented for the authentication procedure is given below.

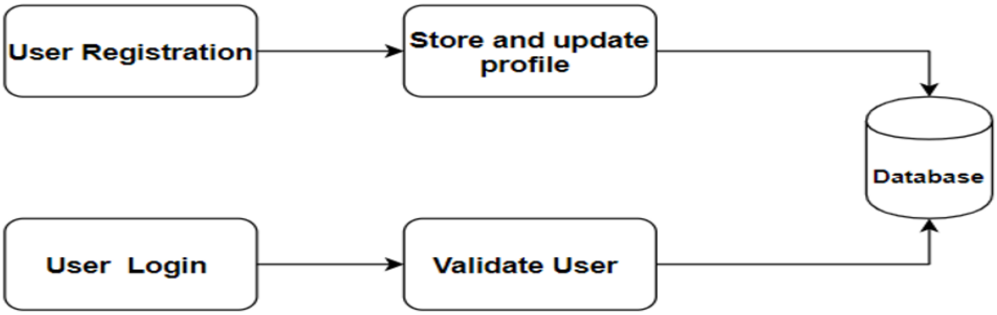


Figure 2. User authentication process

Algorithm 1: User Authentication - {Doctor D, Patient P}

```
Authentication(username(D,P),Password(D,P)){
    String user=username(D,P);
    String pass=password(D,P);
if(user=database.username and password=database.pass){
    grant access(D,P);
    }
else{
    deny access(D,P);
    } }
```

B: Block Creation

The patient consults the doctor, and after the visit, the EHR of the patient will be uploaded as a new block. A new block is created for every visit, and the block is secured using the SHA256 hashing algorithm (Zubaydi et al., 2019). The previous block hash value is obtained whenever a new block is created. Thus, each block contains three segments: the data to be stored, the hash of the block and the hash of the previous block. The first block has no previous block, and hence, it has only the data and hash of the block, called the genesis block. When the next block is created, the previous block hash is calculated, and then a new block is inserted in the blockchain. The process of block creation is shown in Figure 3.

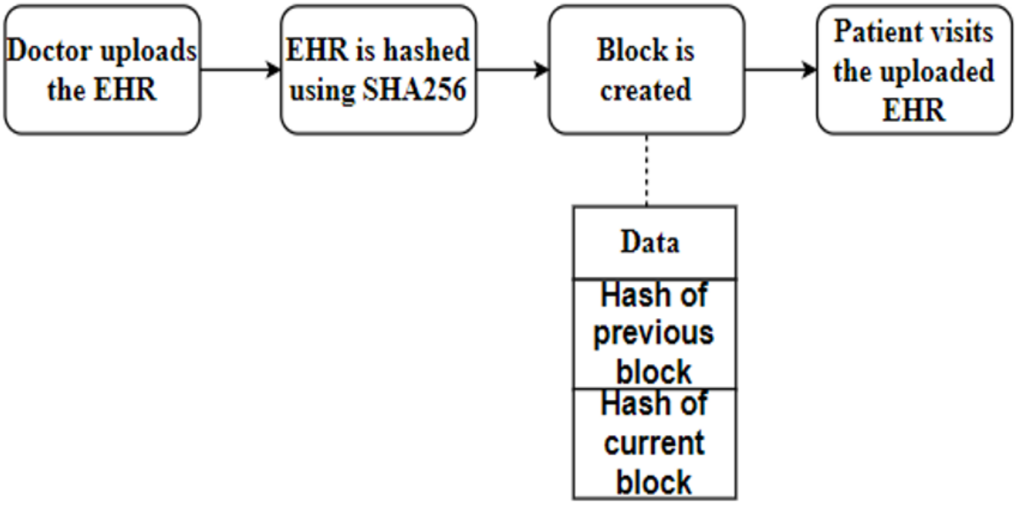


Figure 3. Block creation process

The block created cannot be modified because the hash value will change, making the blockchain immutable. A block ID has been generated for each block, and it is sent to the patient. Whenever the block is retrieved, the transaction details are updated, and a new block is created with reference to the previous hash value. The algorithm takes EHR as input and hashed using a SHA256 hashing algorithm and further converted to hash values.

Algorithm 2: Block creation using SHA256 algorithm

```
INPUT - EHR Record, OUTPUT - Hash of EHR record
Calculate Hash(S string){
    result=hashlib.sha256(str.encode(record))
    record=string(block.index)+block.timestring+block.preblockhash
return calculatedHash(record) }
```

C: Block Validation

As the blockchain is a decentralised network, there are many nodes in the blockchain network with the same copy of blocks. The newly created block has to be updated in all the nodes present in the network. Therefore, an agreement is reached between all nodes using a consensus algorithm and the newly created block is added to the nodes of the blockchain (Zheng et al., 2017). The proposed work employs Delegated Proof of Stake (DPoS) consensus algorithm. In DPoS, there are two types of nodes called consensus nodes and trading nodes. The trading nodes are responsible for creating a block, hashing the block of data, and storing the data block. The consensus node is responsible for validating a block and adding it to the blockchain. There are many nodes in a p2p network, and a consensus node is selected, which is responsible for verifying the block (Yang et al., 2018). After verification, the block is added to the blockchain. The consensus algorithm has three modules: selecting the consensus nodes, verifying blocks, and rejecting the malicious blocks.

For selecting the consensus node, the election process is held. There will be N number of nodes in a network, and a consensus node must be selected. A node conducts the election, and that node sends a broadcast message to all the nodes in the network. After voting, a node with majority votes is selected as the consensus node, which validates the newly created block. As a result, the DPoS algorithm can process the transactions faster and has reduced time complexity compared to Proof of Work (PoW) and Proof of Stake (PoS).

Algorithm 3: Selecting consensus node using Delegated Proof of Stake

```
Broadcast(voting msg){
while(HASH(current Blockhash),HASH(preBlockhash),nounce){
    Broadcast(Nodes)
    nounce = nounce+1}
    Nodes vote for a trusted node
    V(n)=count votes
    Node with max vote = consensus nodes
Node }
End
```

Algorithm 4: Algorithm for reaching consensus

```
Input :block , Output: block good or block error
block←(DATA,HASH(preblockhash,nounce,timestring) if(oldblockindex)!=NewBlockIndex)&&(oldblockhash!=New Block Hash)
    {
broadcast(Block GOOD)
    }
    else{
    broadcast(Block BAD)
    }
```

D: Record Transaction

In the proposed methodology, the patient has complete control and authority over the transaction process of the EHR. The procedure for the EHR transactions between the patient and the doctor is given in Figure 4.

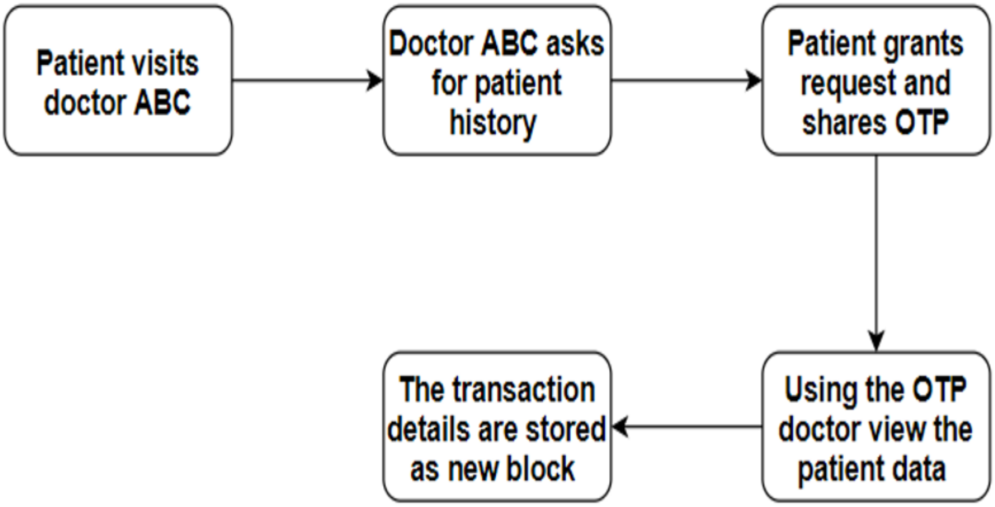

Patient visits doctor ABC
Doctor ABC asks for patient history
Patient grants request and shares OTP
Using the OTP doctor view the patient data
The transaction details are stored as new block

Figure 4. Record transaction process

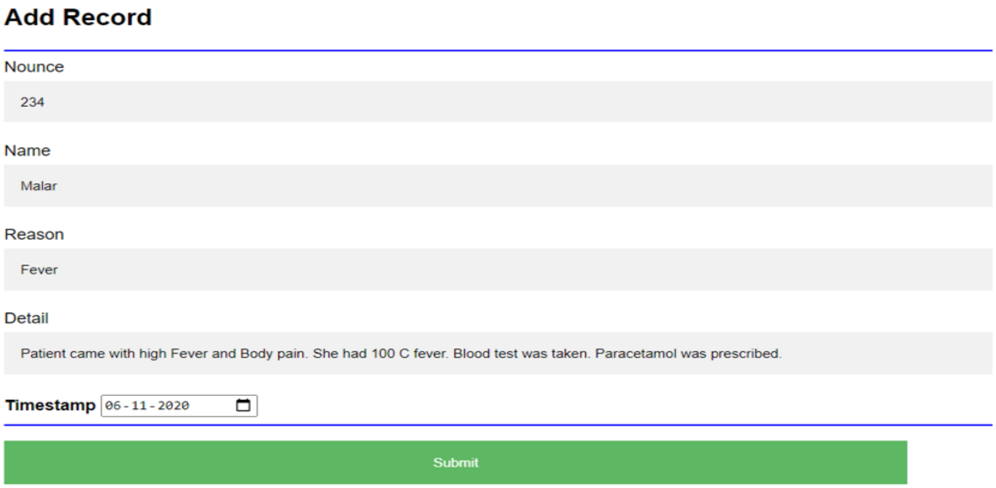
The patient can share the EHR with the doctor, and after consultation, the doctor uploads the EHR. So, whenever a block transaction request is initiated, the patient logs into the account, chooses the transaction option and feeds the doctor's mail ID. The doctor receives OTP to his email. Then the doctor can view the EHR using the received OTP. During the transaction process, the system validates the doctor ID and all the transaction details such as doctor's name, transaction time and block ID are collected and stored in a new block. This block is validated using the DPoS consensus algorithm and added to the blockchain. Finally, the transaction ID is returned to the patient for future reference.

Thus, sharing of EHR among medical practitioners different medical institutions is achievable amidst preserving the privacy of patient's health records. The use of blockchain increases the system's efficiency, reduces the risk of loss of EHR and avoids malicious behaviour in EHR. DPoS is employed for reaching consensus. It is appropriate for applications that need a high level of scalability and hence applied for storing and maintaining EHR in an e-health care system.

RESULTS AND DISCUSSION

The proposed privacy-preserving framework for the EHR using blockchain is mostly developed for healthcare sectors, and it is implemented in this work using Anaconda, Python HTML and MySQL. The user interface is designed using HTML, and the database is set up using MYSQL 5.0.22. The complete system setup has been implemented, and deployed and the performance analysis is done.

A patient can transfer the EHR to any doctor who belongs to a different medical institution. However, only the authorised patients and doctors can access the data, and unauthorised entities will not gain access to patients' medical records.


Add Record

Nounce
234

Name
Malar

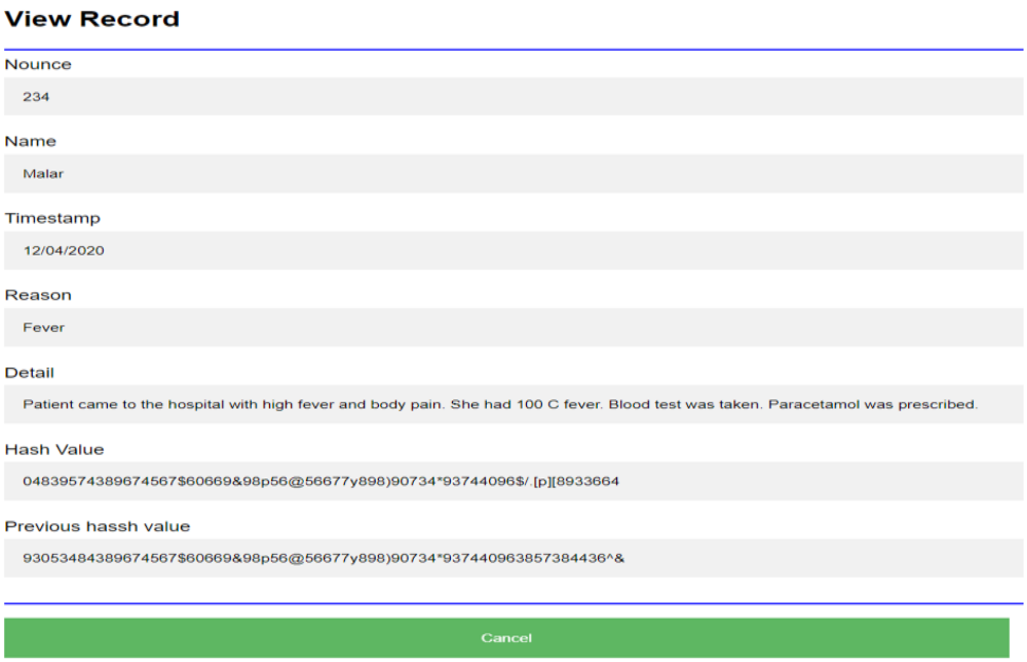
Reason
Fever

Detail
Patient came with high Fever and Body pain. She had 100 C fever. Blood test was taken. Paracetamol was prescribed.

Timestamp 06-11-2020

Figure 5. Doctor adding patient record

Figure 5 shows the log-in page where the doctor logs into his account and fill up the patient details such as patient name, nounce that is a unique value to the block, timestamp that is the date when the block is created. The reason for the visit and the brief description of patient health concerns are given by the doctor. These data are hashed using the SHA256 hashing algorithm, and a block is created.



View Record

Nounce

234

Name

Malar

Timestamp

12/04/2020

Reason

Fever

Detail

Patient came to the hospital with high fever and body pain. She had 100 C fever. Blood test was taken. Paracetamol was prescribed.

Hash Value

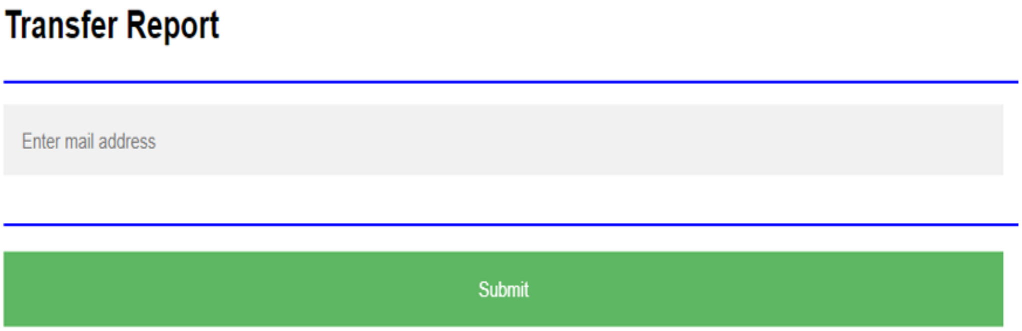
04839574389674567$60669&98p56@56677y898)90734*93744096$/.[p][8933664

Previous hassh value

93053484389674567$60669&98p56@56677y898)90734*937440963857384436^&

Figure 6. Patient viewing medical record

After the doctor uploads the record, the patient can view it by logging in to their respective account. The details such as patient name, nounce, timestamp, hash value, previous block hash values are displayed as depicted in Figure 6.



Transfer Report

Enter mail address

Figure 7. The patient sends a key to the doctor through mail

If a patient wants to send a record to a doctor who belongs different medical institution, then he shares a unique key for that transaction. First, the email ID of the doctor is given then a OTP is generated and sent to the email. The validity for the OTP is for 24 hours and can be used for only one transaction. Finally, the patient mentioning the doctors' email is shown in Figure 7, and an OTP is generated.

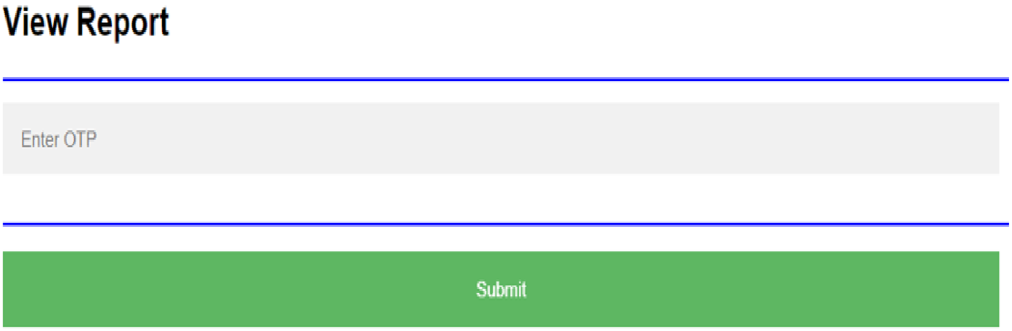
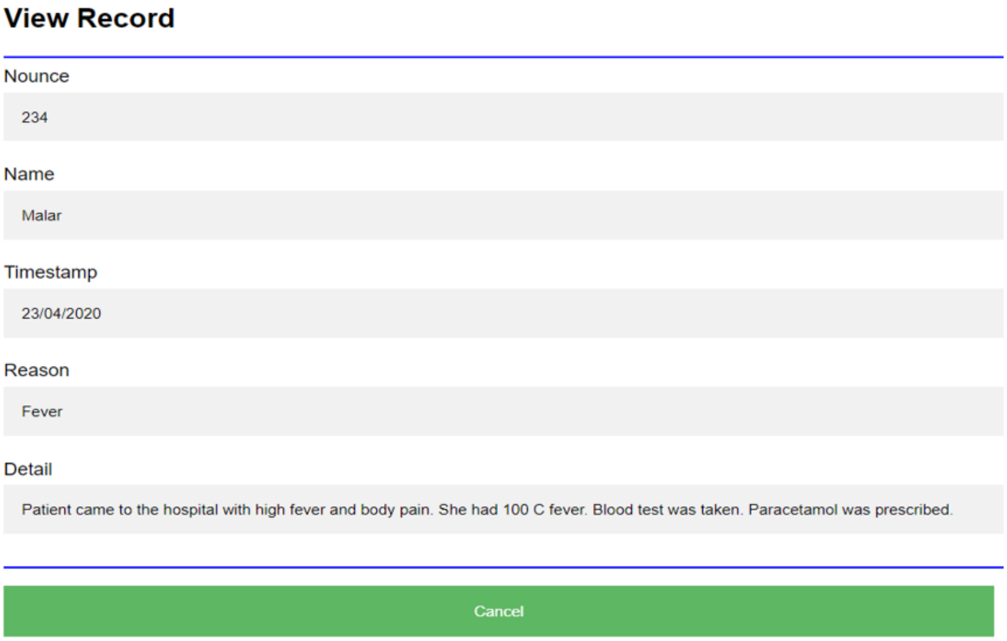


Figure 8. *Doctor enters OTP*

As shown in Figure 8, the OTP received through the doctor's email is entered, and if the OTP is valid, then patient details are displayed at the doctors' end, or an error message will be displayed.


View Record

Nounce
234

Name
Malar

Timestamp
23/04/2020

Reason
Fever

Detail
Patient came to the hospital with high fever and body pain. She had 100 C fever. Blood test was taken. Paracetamol was prescribed.

Figure 9. Viewing patient records by doctor

After successfully validating OTP, the doctor is now allowed to view the patient health record and update the EHR after the consultation. The patient record as viewed and updated by the doctor is shown in Figure 9. After the successful data transaction, details such as doctor's names, time, patient details are collected, and a new block is created. The data has been hashed using SHA256 and validated using Delegated Proof of Stake (DPoS) consensus algorithm. Then the block is added to the blockchain. Likewise, for every transaction, a new block is created and added to the blockchain.

In health care sectors, the transfer of EHR requires an appropriate consensus algorithm with minimum time complexity and cost to reach an agreement between nodes in the block verification process. Hence, the DPoS algorithm is implemented to achieve a high processing speed with reduced expenses compared to PoW and PoS.

Performance Analysis

A. CIA Triad Analysis. *The performance of the proposed architecture is discussed in terms of storage, privacy and security. However, first, we can analyse the CIA triad.*

Confidentiality. Confidentiality of EHR is maintained as the data sharing is done only by the owner of the record (i.e.) the patient. Therefore, the doctors can only view the EHR and upload the EHR after the patient visit. However, the doctor is not permitted to share the EHR with any entity in e-health care.

Integrity. Integrity is the property where no one modifies the stored data without permission. Data integrity is one of the most important characteristics of blockchain, where the data once stored cannot be modified. So, blockchain technology provides 100% integrity for the data present in EHR.

Availability. *A*vailability is managing all hardware software conflicts, thus ensure that the data is available 24/7. Furthermore, since blockchain is a decentralised network it has blocks stored in different P2P networks, which improves data availability.

The proposed system is compared with the existing systems for protecting personal data using blockchain (Zyskind et al., 2015), as given in Table 1.

B. Energy Consumption Analysis. The blockchain network requires many miners, and in PoW, all miners attempt to solve the complex problem, which consumes more energy, but only one can mine a block. As a blockchain network is implemented for preserving the privacy of patient's health records, the energy parameter of PoW and DPoS consensus algorithms are compared. The drawback of the PoW consensus algorithm is that it requires much energy, leading to higher costs, and it can be minimised by choosing the DPoS algorithm.

Table 1

Comparison of Privacy-Preserving Schemes for personal data

Attributes	Privacy-Preserving Data Sharing Framework (Proposed Model)	Decentralising Privacy & Protecting Personal Data (Existing Model)
Privacy Protection	Privacy is ensured through unique keys, and OTP shared for every transaction.	**Adding records, updations and deletions are allowed, which compromises privacy.**
Data Access	Complete access to user's data for both the data owner and shared entity	**Complete access to the data owner and restricted access to the shared entity.**
Data Integrity	Users data cannot be compromised by hacker as the blocks are immutable.	**A small fraction of data can be compromised if hacker gains signing and encryption keys.**
Effectiveness	Efficient for processing data with less time and computation complexity.	**Efficient for storing and processing queries and not for processing data.**
Drawbacks	Less vulnerable to attacks, low energy consumption, low latency.	**More vulnerable to Sybil attacks, excessive energy consumption, High latency.**

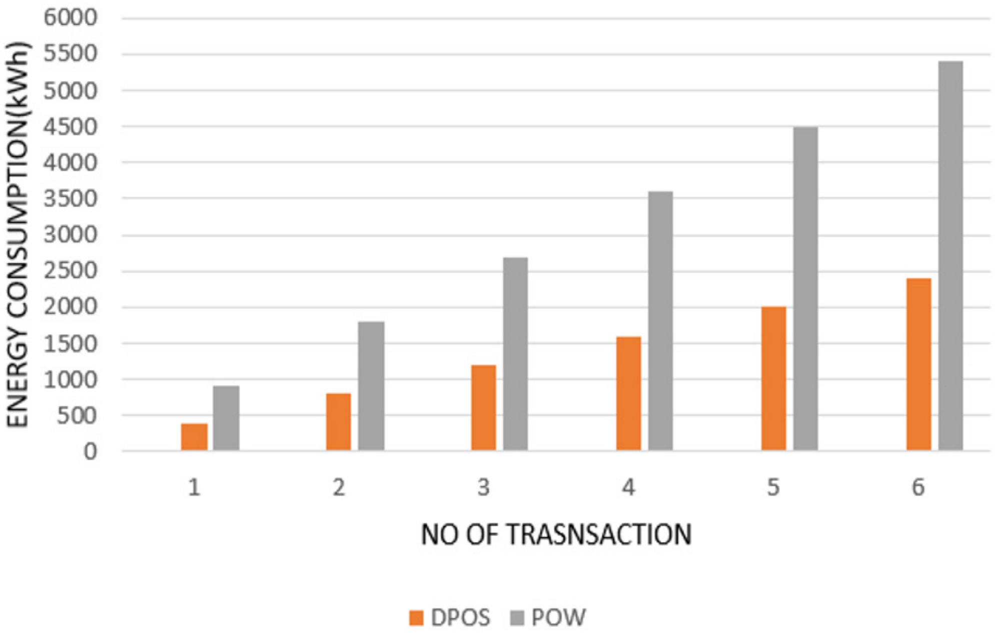


Figure 10. Energy consumption for transaction in PoW vs DPoS

The energy consumption for a record transaction using PoW and DPoS algorithm is given in Figure 10. The PoW consensus algorithm uses more energy to solve a problem as all nodes are involved. The one node that solves the mathematical problem is considered to validate a block. Thus, although one node validates a block, each node in the blockchain works on problem-solving, which leads to high energy consumption and computational capacity.

The energy consumption of the different consensus algorithms differs in terms of the total hash rate of the miners (Borzi & Salim, 2020). It is observed that PoW takes more energy, time and computation power in selecting a consensus node, but in DPoS, the consensus node is selected by a voting algorithm. Hence, applying the Delegated Proof of Stake (DPoS) consensus algorithm reduces the energy consumption by 40%, based on the number of block producers and energy consumed per block producer (Wh).

C. Time Complexity Analysis. The time required for generating and validating a block varies with different consensus algorithms. The existing system uses Proof of Work (PoW) consensus algorithm, and the proposed system implemented the Delegated Proof of Stake (DPoS). Figure 11 shows the time complexity of DPoS consensus algorithm. The average time for generating a block is high for PoW as each node must perform a mathematical calculation for validating a block. However, in DPoS, the validating node is selected based on the voting process that minimises time and cost.

The time complexity of the PoW consensus algorithm is depicted in Figure 12. The PoW algorithm takes 10 minutes to validate a block because of the computation process, whereas in DPoS, no such computation process is needed. Thus 50 blocks can be validated in 10 minutes.

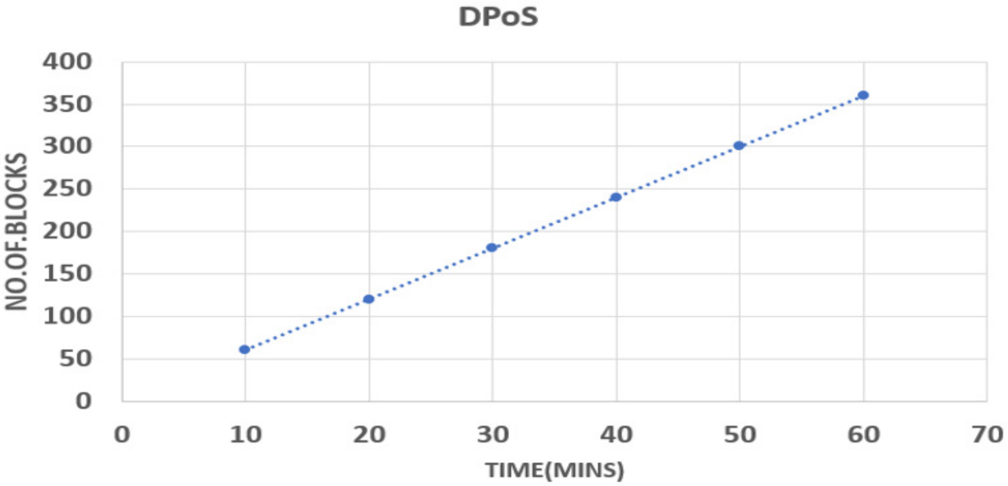


Figure 11. Time complexity of DPoS

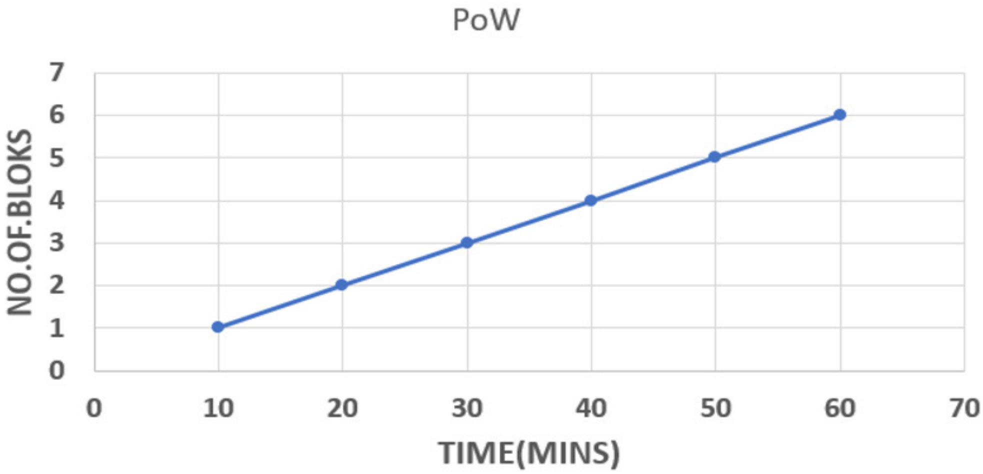


Figure 12. Time complexity of PoW

Table 2 shows the comparison of DPoS and PoW consensus algorithms. The validation node is selected based on the computing power in PoW, but in DPoS, the validating node is selected based on a number of votes. The time and cost are also high for PoW compared to DPoS.

Table 2
Performance of PoW and DPoS

Consensus algorithm	**Proof of work**	**Delegated Proof of Stake**
Basis for assigning accounting rights	Computing power	Stake votes
Resource consumption	High	Low
Average time to generate blocks	10min	5s
Cost	High	Low

CONCLUSION

Blockchain technology is an emerging technology used by most sectors such as banking, healthcare, AI, social media, etc. However, Electronic Health Records (EHR) are stored across different decentralised hospitals, making data-sharing difficult and increasing the risk of patient privacy. In this work, a data sharing framework that employs blockchain technology for storing and retrieving EHR across Medical Institutions is implemented. The decentralisation, transparency and immutability characteristics of blockchain guarantee secure storage and transfer of patients' health records. The EHR is encrypted using the

SHA256 hashing algorithm and stored as a separate block to ensure privacy. The block validation is done using Delegated Proof of Stake (DPoS) consensus algorithm.

In this system, the patient has complete ownership of the health record and is authorised to share the data with any medical practitioner without the intervention of third parties. Hence, the medical data cannot be compromised by any entity that participates in e-health care. The energy consumption and the time complexity are significantly reduced in the proposed model. The future work is to improve the downside of the DPoS consensus algorithm. The DPoS is more centralized, as the master node is responsible for block validation.

ACKNOWLEDGEMENT

The authors would like to thank the Management of B.S.A Crescent Institute of Science & Technology, Chennai, India, for providing the necessary research environment for carrying out this work.

REFERENCES

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE Publishing.* https://doi.org/10.1109/TEMSCON.2017.7998367.

Alhaqbani, B., & Fidge, C. (2008). Privacy-preserving electronic health record linkage using pseudonym identifiers. *In HealthCom 2008-10th International Conference on e-health Networking, Applications and Services (pp. 108-117). IEEE Publishing.* https://doi.org/10.1109/HEALTH.2008.4600120.

Borzi, E., & Salim, D. (2020). *Energy consumption and security in blockchain* (BSc Dissertation). KTH Royal Institute of Technology in Stockholm, Sweden

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical systems, 43*, 5-25. https://doi.org/10.1109/s10916-018-1121-4.

Christidis, K., & Devetsikiotis, M. (2016). Blockchain and smart contract for internet of things. *IEEE Access, 4*, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283-297. http://dx.doi.org/10.1016/j.scs.2018.02.014.

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records. *IEEE Access, 6*, 11676-11686. https://doi.org/10.1109/ACCESS.2018.2801266.

Hossein, K. M., Esmaeili, M. E., Dargahi, T., & Khonsari, A. (2019). Blockchain-based privacy-preserving healthcare architecture. *In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) (pp. 1-4). IEEE.* https://doi.org/10.1109/CCECE.2019.8861857.

Jabeen, F., Hamid, Z., Abdul, W., Ghouzali, S., Malik, S. U. R., Khan, A., Nawaz, S., & Ghafoor, H. (2017). Enhanced architecture for privacy preserving data integration in a medical research environment. *IEEE Access, 5*,13308-13326. https://doi.org/10.1109/ACCESS.2017.2707584.

Jin, H., Lyo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy preserving medical data sharing. *IEEE Access, 7*, 61656-61669. https://doi.org/10.1109/ACCESS.2019.2916503.

Judith, A. G., Mitchel, L., Aleriot, N., & Armani, R. (2018). Electronic health records: An online medical records an asset or a liability under current condition? *Australian Health Review, 42*(1), 59-65. https://doi.org/10.1071/AH16095.

Kadam, S., Meshram, A., & Suryavanshi, S. (2019). Blockchain for healthcare: Privacy preserving medical record. *International Journal of Computers and Applications, 178*(36), 5-9.

Liu, J., Li, X., Ye, L., Zhang, H., & Guizani, M. (2018). BPDS-A blockchain based privacy preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE *Publishing*. https://doi.org/10.1109/GLOCOM.2018.8647713.

Shen, B., Guo, J., & Yang, V. (2019), Medchain: Efficient healthcare data sharing via blockchain. *Applied Sciences*, *9*(6), Article 1207. https://doi.org/10.3390/app9061207.

Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. *In 2018 International Conference on Information Networking (ICOIN) (pp. 473-475). IEEE Publishing.* https://doi.org/10.1109/ICOIN.2018.8343163.

Vedi, A. D., Srivatsava,nG., Dhar, S., & Singh, R. (2019). A decentralised privacy preserving healthcare blockchain for IoT. *Sensors, 19*(2), 326-343. https://doi.org/10.3390/s19020326.

Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., Guo, Y., & Wang, F. (2018). Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Transactions on Computational Social Systems, 5*(4), 942-950. https://doi.org/10.1109/TCSS.2018.2865526.

Xia, Q. I., Sifah, E. B., Assmoah, K. O., Guo, J., & Guizani, M. (2017). Medshare: Trustless medical data sharing among cloud service providers via blockchain. *IEEE Access, 5*,14757-14767. https://doi.org/10.1109/ACCESS.2017.2730843.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N., & Zhou, M. (2018). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access, 7*, 118541-118555. https://doi.org/10.1109/ACCESS.2019.2935149

Zheng, Z., Xie, S., Dai, G., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends*. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE Publishing.* https://doi.org/10.1109/BigDataCongress.2017.85.

Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A review on the role of blockchain technology in healthcare domain. *Electronic*, *8*(6), Article 679. https://doi.org/10.3390/electronics8060679.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE Publishing.* https://doi.org/10.1109/SPW.2015.27.